FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: February 7, 2000	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
MH 11/26/03	AA	5,787,028	07/28/98	Mullin			
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/26/03	AR	R.C. Mullin et al., "Optimal Normal Bases in GF(p^n)*, Discrete Applied Mathematics, 22 (1988/89), pp. 149-161.
	AS	
	AT	

Examiner M. H. Hung	Date Considered 10/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

↑AFFIX CUSTOMER NO. LABEL ABOVE ↑

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: February 7, 2000	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial		Patent Number	Publication Date	Name	Class	Sub-Class	Filing Date
MH 11/20/03	AA	6,252,960 B1	6/26/2001	Serroussi			
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

Examiner Initial		Patent Number	Publication Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Papers, etc.)*

MH 11/20/03	AR	Brouwer et al.; "Doing More with Fewer Bits"; Advances in Cryptology-Asiacrypt' 99, 1999, pgs. 321-332.
	AS	
	AT	

Examiner M. HL Hung	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Attorney Docket: 0225-4188	Serial No.: 09/498,716
Applicant: Lenstra et al.	
Filing Date: 02/07/00	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
MH 11/20/03	AA	4,587,627	05/06/86	Omura			
MH 11/20/03	AB	5,406,628	04/11/95	Beller et al.			
MH 11/21/03	AC	5,481,613	01/02/96	Ford et al.			
MH 11/20/03	AD	4,745,568	05/17/88	Onyszchuk et al.			
MH 11/20/03	AE	4,995,082	02/19/91	Schnorr			
MH 11/20/03	AF	5,231,668	07/27/93	Kravitz			
MH 11/20/03	AG	5,351,297	09/27/94	Miyaji et al.			
MH 11/20/03	AH	5,442,707	08/15/95	Miyaji et al.			
MH 11/20/03	AI	4,405,829	09/83	Rivest et al.			
MH 11/20/03	AJ	4,870,681	09/89	Sedlak			
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
MH 11/20/03	AL	WO 85/01625	04/11/85	WIPO			☐ Yes ☐ No
	AM						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 10/20/03	AR	Neal Koblitz, "A Course in Number Theory and Cryptography," Springer, pp. 87-89, 99-106, 178-182.
MH 11/20/03	AS	Bruce Schneier, "Applied Cryptography", 2e, John Wiley & Sons, Inc., pp. 496-499
MH 11/21/03	AT	P. Duhamel et al., "A Decomposition of the Arithmetic for NTT's with 2 as a Root of Unity," ICASSP '84.
MH 11/21/03	AU	R.L. Rivest et al., "A Method for Obtaining Digital Structures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.
MH 11/21/03	AV	A.K. Lenstra and H.W. Lenstra Jr., "Algorithms in Number Theory", *Handbook of Theoretical Computer Science*, pp. 675-715, 1990.
MH 11/21/03	AW	D. Coppersmith, "Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known", *EUROCRYPT '96, Proceedings*, LNCS 1070, pp. 178-189, 1996.
MH 11/21/03	AX	S. Garfinkel, "PBP: Pretty Good Privacy," 1995, pp. 42-43.

Examiner M. Hal Huang	Date Considered 11/21/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Attorney Docket: 0225-4188	Serial No.: 09/498,716
Applicant: Lenstra et al.	
Filing Date: 02/07/00	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/21/03	AR	Coppersmith and Andrew Odlyzko, "Discrete Logarithms in GF(p)", Algorithmica, Volume 1, No. 1, 1986; pp. 1-15.
MH 11/21/03	AS	Guillou and Quisquater, "Precautions Taken against Various Potential Attacks", Europcrypt '90, Springer 1990, pp. 465-473.
MH 11/21/03	AT	"Information Technology – Open Systems Interconnection – The Directory: Authentication Framework", ITU-T Recommendation X-509, ISO/IEC 9594-8: 1995(E), pp. 1-35. 1995.
MH 11/21/03	AU	Agnew, G.B. et al., "An Implementation for a Fast Public-Key Cryptosystem", Journal of Cryptology, 1991, Vol. 3, pp. 63-79.
MH 11/21/03	AV	Robert D. Silverman, "Fast Generation of Random, Strong RSA Primes", *RSA Laboratories' CryptoBytes*, Vol 3, No. 1, pp. 9-13, Spring 1997.
MH 11/21/03	AW	Ohta et al., (Eds), "Advances in Cryptology", CRYPTO '98, pp. 1-10.
MH 11/21/03	AX	Arjen K. Lenstra, "Generating RSA Moduli with a Predetermined Portion," Advances in Cryptology, ASIACRYPT '98, Beijing, China, Oct. 18-22, 1998; pp. 1-10.

Examiner M. H. Hung Date Considered 11/21/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,719
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/21/03	AR	Guillou, Davio and Quisquater, "Public Key Techniques: Randomness and Redundancy", Cryptologia, 1989, pp. 167-182.
MH 11/21/03	AS	S. Gao and H. Lenstra, "Optimal Normal Bases, Codes and Cryptography," 2, pp. 315-323.
MH 11/21/03	AT	Elwyn R. Berlekamp, "Algebraic Coding Theory" revised 1984 edition, Aegean Park Press, Chapter 10
MH 11/21/03	AU	U.M. Maurer, "Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters", *Journal of Cryptology*, Vol. 8, pg 123-155, 1995.
MH 11/21/03	AV	P.L. Montgomery, "Modular Multiplication Without Trial Division", *Mathematics of Computation*, Vol. 44, No. 170, pp. 519-521, 1985.
MH 11/21/03	AW	Vanstone et al., "Short RSA Keys and Their Generation", Journal of Cryptology, Spring 1995, vol. 8, no. 2, pp. 101-114.
MH 11/21/03	AX	Young, A. et al., "The dark side of "black-box" cryptography or: Should we trust Capstone", Advances on Cryptology," CRYPTO '96, Aug. 18-22, 1996; pp. 89-103.
MH 11/21/03	AY	Vanstone et al., "Using Four-Prime RSA in which some of the Bits are Specified," Electronics Letters, GV, IEE Stevenage, vol. 30, no. 25, 08/12/94, pp. 2118-2119.

Examiner M. Hamlin	Date Considered 11/21/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

#9

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Attorney Docket: 0225-4188	Serial No.: 09/498,716
Applicant: Lenstra et al.	
Filing Date: 02/07/00	Group Art Unit: 2766

U.S. PATENT DOCUMENTS

Examiner Initial	Patent Number	Publication Date	Name	Class	Sub-Class	Filing Date

FOREIGN PATENT DOCUMENTS

Examiner Initial	Patent Number	Publication Date	Country	Class	Sub-Class	Translation
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No
						☐ Yes ☐ No

OTHER DOCUMENTS (continued)

MH 11/20/03	Lenstra et al. "Fast Irreducibility and Subgroup Membership Testing in XTR", Public Key Cryptography, Kim (ed) Springer-Verlag, 2001
MH 11/20/03	Lentra et al. "The XTR Public Key System", (extended version of Crypto 2000 Presentation), pp. 73-86
MH 11/20/03	"Chapter 12. A New Public-Key Cryptosystem" pp. 1-11
MH 11/20/03	"The XTR Cryptosystem", Internet, Sept. 2001, pp. 1-5
MH 11/20/03	More "Letter to DDJ", Doctor Dobb's Journal on CD-Rom, May 1993, pp. 2-3
MH 11/20/03	Smith "Cryptography Without Exponentiation", Dr. Dobb's Journal on CD-Rom, Apr. 1994, pp. 1-3
MH 11/20/03	Smith "LUC Public-Key Encryption", Dr. Dobb's Journal on CD-Rom, Jan. 1993, pp. 1-12
MH 11/20/03	McEliece "Finiate Fields for Computer Scientists and Engineers", Kluwer Academic Publishers, 1987, pp. 96-119
MH 11/20/03	Gong et al. "Public-Key Cryptosystems Based on Cubic Finite Field Extensions", IEEE Transactions on Information Theory, Vol. 45, No. 7, Nov. 1999, pp. 2601-2605
MH 11/20/03	Menezes et al. "Handbook of Applied Cryptography", CRC Press, 1997
MH 11/20/03	Lenstra et al. "Key Improvements to XTR", Asiacrypt, 2000

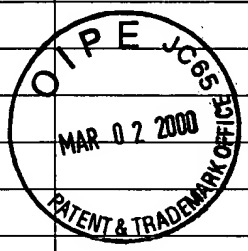
Examiner M. Hanna	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: Unassigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						



FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/20/03	AR	Bailey et al., "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms," Advances in Cryptology, Crypto '98, 18th Annual Int'l Cryptology Conference, August 23-27, pp. 473-485.
MH 11/20/03	AS	Brouwer et al., "Doing More with Few Bits," Advances in Cryptology: Proceedings/ASIACRYPT '99, Int'l Conference on the Theory Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, pp. 321-332.
MH 11/20/03	AT	Cohen et al., "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates," Advances in Cryptology: Proceedings/ASIACRYPT '98, Beijing, Chinga, October 18-22, 1998, pp. 51-65.

Examiner M. H. Hang	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: Unassigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/20/03	AR	Cramer et al. "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," Advances in Cryptology: Proceedings/Crypto '98, 18th Annual Int'l Cryptology Conference, Santa Barbara, Aug. 23-27, 1998; pp. 13-25.
MH 11/20/03	AS	Taher Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, July 1985, pp. 469-472.
MH 11/20/03	AT	P. Gaudry et al., "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," pp. 1-19.

Examiner MH	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: Unassigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 11/20/03	AR	*4.3.3 "How Fast Can We Multiply", Arithmetic, Addison-Wesley Publishing Co., Inc., 1981, pp. 278-281.
MH 11/20/03	AS	Arjen K. Lenstra, "Using Cyclotomic Polynomials to Construct Efficient Discrete Logarithm Cryptosystems over Finite Fields," ACISP '97, Sydney, Australia, July 7-9, 1997, pp. 127-138.
MH 11/20/03	AT	Arjen K. Lenstra, "Generating RSA Moduli with a Predetermined Portion," ASIACRYPT '98, Beijing, Cinga, October 18-22, 1998, pp. 1-10.

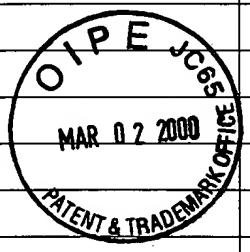
Examiner M. HL Hung	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609.
Draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to Applicant.

FORM PTO-1449 INFORMATION DISCLOSURE CITATION	Attorney Docket: 0225-4188	Serial No.: 09/498,716
	Applicant: Lenstra et al.	
	Filing Date: 02/07/00	Group Art Unit: Unassigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						



FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						☐ Yes ☐ No
	AM						☐ Yes ☐ No
	AN						☐ Yes ☐ No
	AO						☐ Yes ☐ No
	AP						☐ Yes ☐ No

OTHER DOCUMENTS (Including Author, Title, Date, etc.)

MH 1./20/03	AR	Alfred Menezes, "Comparing the Security of ECC and RSA", Alfred Menezes Home Page, supplement to article by B. Schneier, "Elliptic Curve Public-Key Cryptography, Nov. 1999; pp. 1-4.
MH 11/20/03	AS	C.P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, 1981; pp. 161-174.
MH 11/20/03	AT	P. Smith et al., "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," ASIACRYPT'94, November 28 - December 1, 1994; pp. 357-364.

Examiner M. Hill Hung C	Date Considered 11/20/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.